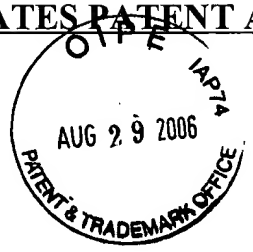
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



In re Application of:

Paul S. Germscheid et al.

Serial No.: 09/448,154 Examiner: L. Wassum

Filing Date: November 24, 1999 Group Art Unit: 2177

For: METHOD AND APPARATUS FOR A WEB APPLICATION SERVER TO PROVIDE FOR WEB USER VALIDATION

Docket No.: 33012/274/101

TRANSMITTAL SHEET

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

CERTIFICATE UNDER 37 C.F.R. 1.8: I hereby certify that this correspondence and the documents described herein are being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 23rd day of August, 2006.

By _____
Carolyn I. Erickson

We are transmitting herewith the attached:

☒ A check in the amount of $500.00 is enclosed.

☐ Small entity status of this application under 37 C.F.R. 1.9 and 1.27 has been established.

☒ Other: Appeal Brief in Triplicate.

☒ Please charge any deficiencies or credit any over payment in the enclosed fees to Deposit Account 14-0620.

By: _____
John L. Rooney
Reg. No. 28,898

NAWROCKI, ROONEY & SIVERTSON, P.A.
Suite 401, Broadway Place East
3433 Broadway Street N.E.
Minneapolis, Minnesota 55413
Telephone: (612) 331-1464
Facsimile: (612) 331-2239

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of	
Paul S. Germscheid et al.	Examiner L. Wassum
Serial No. 09/448,154	Group Art Unit 2177
Filing Date: 11/24/99	
	APPEAL BRIEF
For: METHOD AND APPARATUS FOR A WEB APPLICATION SERVER TO PROVIDE FOR WEB USER VALIDATION	

APPELLANT'S BRIEF
FILED UNDER 37 C.F.R. § 41.37

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

CERTIFICATE UNDER 37 C.F.R. 1.8: I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to the: Commissioner for Patents, Alexandria, VA, 22313-1450 on this 23rd day of August, 20 06.

By Carolyn I. Erickson

This appeal brief is being filed in triplicate within sixty days of the Notice of Appeal mailed June 23, 2006. Permission is

08/30/2006 MGEBREM1 00000025 09448154
01 FC:1402 500.00 OP

hereby granted to charge or credit deposit account number 14-0620 for any errors in fee calculation. Appellants request this Supplemental Appeal Brief be made of record and fully considered.

REAL PARTY IN INTEREST

The Real Party in interest is:

Unisys Corporation

Township Line and Union Meeting Roads

Blue Bell, Pennsylvania 19424

being the assignee of the entire right, title, and interest by all inventors, by way of assignment documents filed at Reel 010421, frame 0627, in the United States Patent and Trademark Office.

RELATED APPEALS AND INTERFERENCES

There are no known pending Appeals and/or Interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal. Therefore, there are no decisions to be placed in the attached Related Proceedings Appendix.

TABLE OF CONTENTS

STATUS OF CLAIMS

The subject patent application was filed on November 24, 1999 containing claims 1-20. Claims 1-3, 6-7, 10-13, and 16-17 have been amended during the course of prosecution in accordance with amendments filed April 25, 2002, November 4, 2002, March 31, 2003, August 29, 2003, December 8, 2003, February 9, 2004, June 24, 2004, October 28, 2004, December 30, 2004, August 4, 2005, January 17, 2006, and April 21, 2006. Dependent claims 4-5, 9-10, 14-15, and 18-20 are appealed in the form as originally presented. Claims 1-20, being all pending claims are presented in the Claims Appendix, attached hereto.

Claims 1-20, being all pending claims have been finally rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison") in view of the article entitled "Access Control in Federated Systems" by De Capitani di Vimercati et al (hereinafter referred to as "De Capitani di Vimercati") and further in view of U.S. Patent No. 6,282,175, issued to Steele et al (hereinafter referred to as "Steele") wherein claims 5, 9-10, 15, and 19-20 have been rejected further in view of the article "Unisys CSG

MarketPlace -- The MAPPER System" (hereinafter referred to as "Unisys".

STATUS OF THE AMENDMENTS

Applicant has filed responses to official actions on April 25, 2002, November 4, 2002, March 31, 2003, August 29, 2003, December 8, 2003, February 9, 2004, June 24, 2004, October 28, 2004, December 30, 2004, August 4, 2005, January 17, 2006, and April 21, 2006. Of these submissions, all pertinent amendments have been made to the claims. The amendment after final filed April 21, 2006, was entered by the Examiner by way of Advisory Action mailed May 23, 2006. This amendment disposed of the rejections under 35 U.S.C. 112.

AS a result, claims 1-20, recorded herewith as Claims Appendix, are in the form of April 21, 2006 following submission of the last presented amendment to the claims.

SUMMARY OF CLAIMED SUBJECT MATTER [1]

The present invention generally relates to data base management systems and more particularly relates to enhancements for providing secure access to data base management systems via Internet user terminals[2]. The present invention overcomes the disadvantages of the prior art by providing a method of and apparatus for utilizing the power of a full featured data base management system by a user at a world wide web browser coupled to the world wide web or Internet while maintaining security[3]. Security has typically involved either the encryption of sign on information, or else the using of secure connections requiring more administrative setup. To make access to a proprietary data base by Internet users practical, a sophisticated security system is required to prevent intentional or inadvertent unauthorized access to the sensitive data of an organization[4].

In order to permit any such access, the present invention has a security feature that requires a user to sign on with a UserID

---

[1] The references to the specification and drawings provided herein are only exemplary and are not deemed to be limiting. The purpose of the references is to enable the Board to more quickly determine where the claimed subject matter is described within the present application.
[2]See Specification at page 3 lines 3-5.
[3]See Specification at page 7, lines 3-5.
[4]See Specification at page 7, lines 6-9.

and Password when secured services are requested. This invention will provide a new SignOn capability which allows for site-specific data to be used to identify a user. The site-specific data is converted to a valid UserID/Password by a User Validation service implemented by a site. This feature requires a site to implement a site-user. The site must also implement a User Validation service. This service will return data in a pre-defined format so that it can be processed[5].

This unique User Validation feature provides the capability for the browser to send information, which is then translated into a UserID/Password on the Cool ICE Web Application server. This bypasses the need to send a UserID/Password from browser to server, which enhances security[6].

Such a security system should provide multiple levels of access to accommodate a variety of authorized user categories. Site specific profiles may offer only limited or no access to sensitive data when the user terminal site is not particularly secure. These features can be effectively combined with physical security procedures to provide many specialized security profiles. Each individual service within an ASP may be validated. Other solutions must still transmit sign on over the network for each

---

[5]See Specification at page 7, lines 9-15.
[6]See Specification at page 7, lines 16-19.

service. Even though such transmissions may be encrypted or sent over a secure connection, they can still be susceptible to being accessed and decrypted by malicious users. The present approach enhances granularity of security. The UserValidation service is used to convert site specific user validation data to a UserID and Password[7].

From the system perspective, rather than defining several levels of data classification, the different classes of users and user sites are managed by identifying a security profile as a portion of those service requests requiring access to secure data. Thus, the security profile accompanies the data/service to be accessed. The user simply need execute the sign on procedure which correlates to the access permitted. This permits certain levels of data to be accessed by one or more of the several classes of user[8].

In the preferred mode of practicing the present invention, a user signs on to the gateway with a generic login protocol providing access as an unsecured user. All users of the gateway sign on in a similar fashion. Should the user request access to a secure function or to secure data, the user validation, rather than the secure service, manages the security profiling technique. The service request for secure access results in the user validation

---

[7]See Specification at page 7, line 20,. through page 8, line 6.
[8]See Specification at page 8, lines 7-12.

requesting such additional logon information as is required to permit the desired access. In this way, the web browser request is associated with security attributes so that each web user transaction attaches to the database management system object using the security obtained from the Cool ICE session object[9].

The present invention adds a Access restriction. That is, web applications may be written to require a secured sign on in order to access particular service. A UserID and Password is required to access the service in order to identify a user with the proper security. Often times his UserID and Password is associated with a database that can allow access to sensitive information beyond what the web application server is accessing[10].

Typically this UserID and Password is entered in a web browser page, and transmitted across the network to the application server which then uses this sign on information to access the service. This may cause a security breach, as network packets may be intercepted, and the sign on information compromised. The invention enhances security in that sign on information is only processed at the application server, and no sign on information is transmitted over a network[11].

---

[9]See Specification at page 8, lines 13-20.
[10]See Specification at page 8, line 21, through page 9, line 2.
[11]See Specification at page 9, lines 3-7.

The transaction data in HTML format received by the server from the user, along with the state information stored in the repository, are processed by a service handler into a sequence of service requests in the command language of the data base management system[12].

Through the use of the repository to store the state of the service request sequence, the service handler to execute data base management commands, the world wide web user is capable of performing each and every data base management function available to any user. In addition, the data base management system user at the world wide web terminal is able to accomplish this without extensive training concerning the command language of the data base management system[13].

Claims 16 and 18 are the only pending claims having "means-plus-function" limitations. Claim 16 has four such limitations which are correlated to Applicants' disclosure as follows:

a) "permitting means"[14];

b) "offering means"[15];

c) "providing means"[16]; and

---

[12]See Specification at page 9, lines 8-10.
[13]See Specification at page 9, lis 11-15.
[14]See Specification at page 16, lines 3-6 and Fig. 3, Client 46.
[15]See Specification at page 16, lines 7-12 and Fig. 3, Web Server 50.
[16]See Specification at page 10, line 19, through page 22, lines 8-11, and Fig. 5, Cool ICE Administration 104.

d) "preventing means"[17].

Claim 18 has a single "means-plus-function", called "transmitting means". This element is defined in part at Fig. 5, Web Browser 92, and page 21, lines 3-6, of the specification.

Claims 17 and 19-20 which depend from independent claim 16 present no additional "means-plus-function" limitations.

[17]See Specification at page 22, lines 3-8, and Fig. 5, Cool ICE Service Handler 102.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Are claims 1-4, 6-8, 11-14, and 16-18 unpatentable under 35 U.S.C. 103(a) as being obvious over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison") in view of the article, "Access Control in Federated Systems" (hereinafter referred to as "De Capitani di Vimercati") and further in view of U.S. Patent No. 6,282,175, issued to Steele et al. (hereinafter referred to as "Steele")?

I1. Are claims 5, 9-10, 15, and 19-20 unpatentable under 35 U.S.C. 103(a) as being obvious over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison") in view of the article, "Access Control in Federated Systems" (hereinafter referred to as "De Capitani di Vimercati") in view of U.S. Patent No. 6,282,175, issued to Steele et al. (hereinafter referred to as "Steele") and further in view of the article, UNISYS CSG MarketPlace -- The MAPPER System (hereinafter referred to as "Unisys")?

ARGUMENT

I. Claims 1-4, 6-8, 11-14, and 16-18 are not unpatentable under 35 U.S.C. 103(a) as being obvious over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison") in view of the article, "Access Control in Federated Systems" (hereinafter referred to as "De Capitani di Vimercati") and further in view of U.S. Patent No. 6,282,175, issued to Steele et al. (hereinafter referred to as "Steele").

MPEP 2143 specifies the three required showings for the Examiner to make a *prima facie* case of obviousness. These requirements are: 1)motivation to make the alleged combination; 2)reasonable likelihood of success of the alleged combination; and 3)all claim elements in alleged combination. The Examiner has not met his burden with regard to any of these three required showings and therefore has not presented a *prima facie* case of obviousness. The rejection of claims 1-4, 6-8, 11-14, and 16-18 should be

reversed for failure of the Examiner to present a *prima facie* case of obviousness.

In attempting to make the required showing of motivation, the Examiner has provided three positions associated with the motivation to combine Garrison with De Capitani di Vimercati. The first of these simply alleges that the references are in the same field of endeavor. The Examiner is well aware of that this is inadequate to meet the requirements of MPEP 2143, because the "field of endeavor" contains a plethora of material which is irrelevant, incompatible, and representative of alternative approaches.

In his second position, the Examiner states:

> .....whereby the user identifier need not be transmitted on a publicly accessible digital communication network (i.e. global authentication), since (sic) **the alternative would be to impose local authentication**..... (emphasis added)

This statement is absolutely inconsistent with Garrison, which teaches encryption of the identifier at column 3, lines 3-8. The reader of Garrison would specifically be taught that the user identifier should be transmitted in an encrypted form. Therefore, the Examiner's statement is deemed clearly erroneous.

In his third argument, the Examiner states:

> ....since (sic) without such a mechanism all objects would necessarily have the same level of access.

Again, this statement is clearly erroneous on its face. Garrison is only one of the references within the present record which provide multiple "levels" of access without the "mechanism" of De Capitani di Vimercati for changing access levels. Thus, as admitted by the Examiner, the alleged combination of De Capitani di Vimercati would actually reduce, rather than increase the security flexibility of Garrison.

As a result, the Examiner has failed to show motivation to combine De Capitani di Vimercati with Garrison as based upon legally irrelevant and clearly erroneous findings of fact.

The Examiner similarly fails in his attempt to show the motivation for the further combination with Steele. He states in part:

> ....since (sic) upon receipt of the service request the request can be satisfied merely by executing the corresponding predefined command language script (see Steele et al, col. 7, lines 35-56), without the necessity to first translate the request into a valid SQL command and then submit the SQL command to the database (as is the case in Garrison, col. 8, lines 9-19).

It is absolutely baffling why the Examiner would consider this to show motivation. There is no allegation that the approach of Steele is superior or would provide any additional benefits. Whereas combining De Capitani di Vimercati with Garrison would actually decrease the capability of the alleged combination as explained above, the further combination with Steele is not

motivated, because it would offer no further capability. The Examiner again has failed to show motivation.

The Examiner has not made any showing of reasonable likelihood of success, perhaps relying upon his former statements on the matter. The record contains the Examiner's previous finding of reasonable likelihood of success which provides in part:

> As stated in the previous Office action, in the field of computer programming, **success is assured** in the incorporation of a feature into a piece of software. (Emphasis added)

This statement is clearly erroneous, because it does not account for differences in hardware, software, and system architectures. Most simply, when one purchases a software package, the labeling typically lists "system requirements". In other words, that software package cannot be run on a given system unless it comports with those "system requirements". For more complex "real time" applications, differences in hardware, software, operational philosophy, and system architectures become critical.

It seems most convenient to address the requirement of MPEP 2143 to show all claim elements within the alleged combination by direct referral to each of the claims.

I.A. Claim 1 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 1 is limited by:

> an administration module located within said data base management system for permitting a manager having authority to access said administration module to associate a particular security level which each of said plurality of service requests

The Examiner ignores the claimed limitations and instead states:

> "The federated administrator specifies global authorizations to access the federated data [and t]he local administrator specifies authorizations to access the local objects".

Clearly, the Examiner ignores the claimed element of "an administration module" which is a "thing" and prefers to discuss the actions taken by "people" (i.e., federated administrator and local administrator). Because De Capitani di Vimercati does not explain how the discussed people perform these tasks, it is clear that the claimed "administration module" is not (and can not be) present in the prior art.

Furthermore, the claimed invention requires the claimed "administration module" to "associate a particular security level which each of said plurality of **service requests**". As explained above in the Summary of the Claimed Subject Matter, the security profile may be associated with "function" rather than just specific "data". That is radically different from controlling "access" to data as found in De Capitani di Vimercati. For example in Applicants' invention, a particular site can be authorized to read

certain data but be unauthorized to modify that same data. According to De Capitani di Vimercati, if access is granted, a user can both read and modify data, whereas if access is not granted, the user can neither read nor modify that data.

Therefore, the rejection of claim 1, and all claims depending therefrom, is should be reversed for failure of the Examiner to present a *prima facie* case of obviousness as required by MPEP 2143.

I.B. Claim 2 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

In his rejection of claims 2 and 13, the Examiner states:

> Regarding claims 2 and 13, De Capitani di Vimercati et al. additionally teaches a data processing environment wherein a security profile is **generated by said data management system**. (Emphasis added)

This finding is clearly erroneous and specifically contradicted by the Examiner. He further states:

> "The **federated administrator specifies** global authorizations to access the federated data [and t]he **local administrator specifies** authorizations to access the local objects". (emphasis added)

Thus, the Examiner states that when the "federated administrator specifies" or the "local administrator specifies", that this is the same as the claimed **generated by said data management system**. This finding is clearly erroneous. The rejection of claim 2, and any

claim depending therefrom, is should be reversed as based upon inconsistent and clearly erroneous findings of fact and failure to comply with MPEP 2143.

I.C. Claim 3 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 3 depends from claim 2 and requires a particular service request to include a site-specific user-id. In Applicants' claimed invention, the site-specific user-id must be transferred with the service request to impart greater granularity of security profiling, as explained above. A given user may be authorized to make certain service requests but not others. In general, most users will not be authorized to make all service requests. This is not found in the alleged combination. The rejection of claim 3 should be reversed as based upon clearly erroneous findings of fact.

I.D. Claim 4 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 4 depends from claim 3 and further limits the publicly accessible digital data communication network. As such it presents a new and unique combination not found in the prior art of record.

The rejection of claim 4 should be reversed for failure of the Examiner to present a *prima facie* case of obviousness.

I.E. Claim 6 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 6 is an independent apparatus claim. The third claimed element reads:

> an administration module located within said data base management system which may be utilized by a manager having authority to access said administration module to assign a particular security level to each of said plurality of service requests;

The alleged combination does not meet this limitation as explained above, because the alleged combination does not contain "an administration module", and the alleged combination controls access to data rather than the claimed use of "service requests". Therefore, the rejection of claim 6, and all claims depending therefrom, should be reversed for failure of the Examiner to make a *prima facie* case of obviousness as specified by MPEP 2143.

I.F. Claim 7 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 7 depends from claim 6 and is further limited by "wherein said terminal accesses said data base by transferring said

service request to said data base management system". Misquoting Applicants' claimed invention by stating "data entity" rather than the claimed "data base", the Examiner cites Garrison column 6, line 60, through column 7, lines 32, and column 7, line 50, through column 8, line 37. Neither of these citations has even mentions a "service request". Though the term, "service request", has standard usage in the art, a working definition is provided by Applicants at page 25, lines 11-16, as:

> The service request itself is utilized by Cool ICE service handler 156 to retrieve a previously stored sequence of data base management system command statements from repository 166. Thus, in the general case, a single service request will result in the execution of a number of ordered data base management system commands. The exact sequence of these commands is defined by the service request developer as explained in more detail below.

The rejection of claim 7 should be reversed as based upon clearly erroneous findings of fact.

I.G. Claim 8 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 8 requires a particular service request to include a site-specific user-id. In Applicants' claimed invention, the site-specific user-id must be transferred with the service request to impart greater granularity of security profiling. A given user may be authorized to make certain service requests but not others. In

general, most users will not be authorized to make all service requests. This is not found in the alleged combination. The rejection of claim 8 should be reversed as based upon clearly erroneous findings of fact.

I.H. Claim 11 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 11 is an independent method claim having seven steps. The fifth step requires "requesting said first identifier from said user terminal". Not only is this step not found in the alleged combination, the Examiner completely ignores the limitation. He does not even mention the existence of the limitation even though it has been of record since at least August 4, 2005. Therefore, the rejection of claim 11, and all claims depending therefrom, should be reversed for failure of the Examiner to make a *prima facie* case of obviousness as specified by MPEP 2143.

I.I. Claim 12 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 12 requires a particular service request to include a site-specific user-id. In Applicants' claimed invention, the site-specific user-id must be transferred with the service request to

impart greater granularity of security profiling. A given user may be authorized to make certain service requests but not others. In general, most users will not be authorized to make all service requests. This is not found in the alleged combination. The rejection of claim 12 should be reversed as based upon clearly erroneous findings of fact.

I.J. Claim 13 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

In his rejection of claim 13, the Examiner states:

> Regarding claims 2 and 13, De Capitani di Vimercati et al. additionally teaches a data processing environment wherein a security profile is **generated by said data management system**. (Emphasis added)

This finding is clearly erroneous and specifically contradicted by the Examiner. He further states:

> "The **federated administrator specifies** global authorizations to access the federated data [and t]he **local administrator specifies** authorizations to access the local objects". (emphasis added)

Thus, the Examiner states that when the "federated administrator specifies" or the "local administrator specifies", that this is the same as the claimed **generated by said data management system**. This finding is clearly erroneous. The rejection of claim 13, and any

claim depending therefrom, should be reversed as based upon clearly erroneous findings of fact and failure to comply with MPEP 2143.

I.K. Claim 14 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 14 depends from claim 13 and further limits the publicly accessible digital data communication network. As such it presents a new and unique combination not found in the prior art of record. The rejection of claim 14 should be reversed.

I.L. Claim 16 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 16 is an independent apparatus claim having means-plus-function limitations. Claim 16 contains the element, "providing means located within said offering means for providing an authorized manager to assign a particular security level to each of said data processing services". As explained above, this element is not found in the alleged combination. Therefore, the rejection of claim 16, and all claims depending therefrom, should be reversed for failure of the Examiner to make a *prima facie* case of obviousness as specified by MPEP 2143.

I.M. Claim 17 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 17 depends from claim 16 and further limits the publicly accessible digital data communication network. As such it presents a new and unique combination not found in the prior art of record. The rejection of claim 17 should be reversed.

I.N. Claim 18 is not unpatentable over Garrison in view of De Decapitani di Vimercati and further in view of Steele.

Claim 18 requires a particular service request to include a site-specific user-id. In Applicants' claimed invention, the site-specific user-id must be transferred with the service request to impart greater granularity of security profiling. A given user may be authorized to make certain service requests but not others. In general, most users will not be authorized to make all service requests. This is not found in the alleged combination. The rejection of claim 18 should be reversed as based upon clearly erroneous findings of fact.

I1. Claims 5, 9-10, 15, and 19-20 are not unpatentable under 35 U.S.C. 103(a) as being obvious over U.S. Patent No. 6,275,939, issued to Garrison (hereinafter referred to as "Garrison") in view

of the article, "Access Control in Federated Systems" (hereinafter referred to as "De Capitani di Vimercati") in view of U.S. Patent No. 6,282,175, issued to Steele et al. (hereinafter referred to as "Steele") and further in view of the article, UNISYS CSG MarketPlace -- The MAPPER System (hereinafter referred to as "Unisys").

To the untenable alleged combination of Garrison, De Capitani di Vimercati, the Examiner alleges the further combination with Unisys. None of Garrison, De Capitani di Vimercati, nor Steele even mentions a "data base management system". Therefore, it makes no sense for the Examiner to allege that one of skill in the art would be motivated to combine the teachings of UNISYS with Garrison, De Capitani di Vimercati to provide it with a particular data base management system. Lacking motivation, it is extremely apparent that there is no reasonable likelihood of success of the alleged combination without the teachings of Applicants.

Furthermore, there is certainly no indication that there is any reasonable likelihood of success of the alleged combination. In fact, the record specifically shows that such a combination would not be operable. The Specification at page 3, lines 12-13, states:

> The MAPPER system, which runs on various hardware platforms also available from Unisys Corporation. . . . .

Thus, MAPPER would not run on the hardware platforms of Garrison, De Capitani di Vimercati, and Steele.

The rejection of claims 5, 9, 10, 15, 19, and 20 is respectfully traversed for failure of the Examiner to make a *prima facie* case of obviousness.

CONCLUSION

Having thus reviewed the final rejections of claims 1-20, being all pending claims, it seems abundantly clear that the limitations of these claims are not unpatentable in view of the prior art of record. Thus, the rejection of these claims should be reversed as being based upon clearly erroneous fact findings and errors of law.

Respectfully submitted

Paul S. Germscheid et al.

By their attorney,

Date August 23 2006

John L. Rooney
Reg. No. 28,898
Suite 401,Broadway Place East
3433 Broadway Street N.E.
Minneapolis, MN 55413
(612) 331-1464

CLAIMS APPENDIX

1. In a data processing environment having a user with a first user identifier, which uniquely identifies said user, at a terminal located at a particular site, the improvement comprising:

a. wherein said terminal includes a second user identifier which uniquely identifies said particular site and wherein said user utilizes said terminal to generate a particular one of a plurality of service requests the honoring of which requiring access to secure data responsively coupled via a publically accessible digital data communication network to a data base management system having at least one data base containing said secure data which honors said particular one of said plurality of service requests by executing a sequence of command language script corresponding to said particular one of said plurality of service requests;

b. an administration module located within said data base management system for permitting a manager having authority to access said administration module to associate a particular security level which each of said plurality of service requests; and

c. a security profile indicative of said particular security level maintained by said administration module and stored in

association with said sequence of command language script corresponding to said sequence of command language script whereby said data base management system permits said user to access said secure data from said at least one data base from said terminal at said particular site without transfer of said first user identifier uniquely identifying said user via said publically accessible digital data communication network if said second user identifier corresponds to said security profile.

2. The improvement according to claim 1 wherein said security profile is generated by said data base management system.

3. The improvement according to claim 2 further comprising a portion of said second user identifier whereby said data base management system is notified that said second user identifier corresponds to said particular site rather than corresponding to said user.

4. The improvement according to claim 3 wherein said publically accessible digital data communication network further comprises the Internet.

5. The improvement according to claim 4 wherein said data base management system is MAPPER.

6. An apparatus comprising:

a. a terminal located at a particular location having a first identifier which uniquely identifies said terminal and a user with a second identifier which uniquely identifies said user and which generates a particular one of a plurality of service requests;

b. a data base management system having access to a data base responsively coupled to said terminal via a publically accessible digital data communication network and which executes a sequence of command language script to honor said particular one of said plurality of service requests;

c. an administration module located within said data base management system which may be utilized by a manager having authority to access said administration module to assign a particular security level to each of said plurality of service requests; and

d. a security profile generated by said data base management system corresponding to said sequence of command language script whereby said data base management system executes said sequence of command language script to provide access to a

particular secure portion of said data base corresponding to said location specific security profile without transfer of said second identifier via said publically accessible digital data communication network if said first identifier corresponds to said security profile.

7. The apparatus of claim 6 wherein said terminal accesses said data base by transferring said particular one of said plurality of service requests to said data base management system.

8. The apparatus of claim 7 wherein said first identifier further comprises a special portion corresponding to said particular location.

9. The apparatus of claim 8 wherein said data base management system further comprises MAPPER.

10. The apparatus of claim 9 wherein said publically accessible digital data communication network further comprises the world wide web.

11. A method of utilizing a terminal having a first identifier and having a user with a user identifier which uniquely identifies said

user located at a particular site to securely access a remote data base management system having a data base via a publically accessible digital data communication network comprising:

a. signing on to said terminal by said user utilizing said user identifier;

b. transmitting a service request requiring execution of a sequence of command language statements to provide secure access to said data base from said terminal without transferring said user identifier;

c. receiving said service request by said remote data base management system;

d. determining a security profile corresponding to said sequence of command language statements utilizing an administration module by a manager having authority to access said administration module;

e. requesting said first identifier from said user terminal;

f. comparing said security profile with said first_identifier; and

g. honoring said service request if and only if said first identifier corresponds to said security profile.

12. A method according to claim 11 wherein said transmitting step further comprises transmitting a portion of said first identifier identifying said particular site.

13. A method according to claim 12 wherein said determining step further comprises generating said security profile corresponding to said sequence of command language statements.

14. A method according to claim 13 wherein said publically accessible digital data communication network further comprises the Internet.

15. A method according to claim 14 wherein said remote data base management system further comprises the MAPPER data base management system.

16. An apparatus comprising:

a. permitting means located at a site having a first identifier for permitting a user having a user identifier to interact with a data base responsively coupled via a publically accessible digital data communication network;

b. offering means responsively coupled to said permitting means via said publically accessible digital data communication network

for offering data processing services involving access to said data base in response to said service request by executing a sequence of command language script;

c. providing means located within said offering means for providing an authorized manager to assign a particular security level to each of said data processing services; and

d. preventing means responsively coupled to said offering means and said providing means for preventing said offering means from offering said data processing services to said user in response to said service request unless said site corresponds to a security profile associated with said particular security level assigned by said authorized manager to said sequence of command language script and maintained by said administration module wherein said security profile permits access to said data base without access to said user identifier.

17. An apparatus according to claim 16 wherein said publically accessible digital data communication network further comprises the Internet.

18. An apparatus according to claim 17 wherein said permitting means further comprises means for transmitting a portion of said first identifier corresponding to said site.

19. An apparatus according to claim 18 wherein said offering means further comprises MAPPER data base management system.

20. An apparatus according to claim 19 wherein said permitting means further comprises an industry standard personal computer.

EVIDENCE APPENDIX

There is no evidence or documents deemed appropriate to be included within this Appendix.

RELATED PROCEEDINGS APPENDIX

There are no decisions or other papers deemed appropriate to be included in this Appendix.